Subject	Date Last Reviewed	Policy #
Remote Access Policy	October 2021	ITS – 5.0
	Application	**Supersedes**
	ITS Security	
	Distribution	
	All Departments	
Recommended	**Approved**	
Preston D. Marx, VP Information Systems	James I. Marshall, President & CEO	

1.0 Purpose

This policy defines the standards and procedures for remote access to UBH network resources.

2.0 Scope

The policy applies to all areas of remote access to the UBH local network. Remote access is defined in this policy as any access from a device on a Non-UBH controlled network seeking access to the UBH internal network. These users could be employees, consultants, vendors or remote clinics.

3.0 Policy

Overview

The greatest exposure for an organization or a user is when data packets are passed between two end devices. Personal data, sensitive corporate data, and passwords may be passed over the network and are vulnerable to interception or misuse. To reduce the likelihood of this occurring, UBH has established an encrypted communications link through a virtual private network (VPN).

Remote Access

There are many instances where remote access to UBH resources makes business sense. These communications must always utilize a VPN. UBH maintains a VPN concentrator appliance that manages these connections ensuring only authorized users are granted access. Remote access is given by request from a department manager to the ITS team.

EXHIBIT 6

UBH Responsibilities
The Uintah Basin Healthcare ITS team must ensure corporate firewalls and other security appliances are running the latest stable code and have appropriate rules in place to safeguard the internal network. The ITS team will review remote access in conjunctions with the audit prescribed in the Employee Account Policy.

Remote access is not given to any role or position by default. The access is granted when a business need is displayed. Whenever possible remote access should be limited to UBH provided computers where local safeguards are updated and in place. Access through the VPN will be limited to only those resources needed by the user.

User Responsibilities
Access to UBH resources remotely is a feature meant to increase productivity, promote mobility and improve operations. All VPN access is password protected and follows the same guidelines in the Password Policy.

As stated above, whenever possible remote access should be limited to UBH provided computers where local safeguards are updated and in place. UBH issued computers are primarily for work use only and should not be used by unauthorized users. If a user is using a VPN from another device not issued by UBH ITS, it is the responsibility of the user to ensure that that machine and its network are secure and free from any malicious or harmful programs.

Resources not located on UBH network
There are many applications and resources where a user has direct access without establishing a VPN with Uintah Basin Healthcare. These applications do not reside on the UBH network locally, but are remotely hosted, cloud-based solutions. These applications are most secure when accessed from the UBH network and should be whenever possible. When accessing a remote hosted solution, ensure your web browser is updated and that the site is using SSL encryption. All activity on these applications, regardless of your location, is under the same HIPPA and ITS guidelines as if you were on premise.

Violations
Uintah Basin Healthcare takes threats to their internal network seriously. Anyone found doing activities that are a threat to the network, create a hole in security or are circumventing UBH security measures will be subject to corrective action up to and including termination. If necessary, Uintah Basin Healthcare also reserves the right to advise appropriate legal officials of any illegal violations.